

Data Privacy Checklist

Six Practical Steps to Strengthen Your Business Today



A Non-Technical Guide to Smarter, Safer Data Practices

Customer data, supplier records, and internal information are valuable—and vulnerable. Taking proactive steps to protect them doesn't just prevent breaches; it builds trust, supports compliance, and keeps your business resilient.

1. Review Who Has Access to Your Data

- **Why it Matters:** Too many people having access increases the risk of accidental or malicious exposure.
- **Action steps:**
 - Check which employees, contractors, or third parties can access your systems, files, and platforms.
 - Remove or restrict access for former staff or anyone who doesn't need it.
 - Use role-based permissions so people only access what's relevant to their job.

2. Enable Multi-Factor Authentication (MFA)

- **Why it Matters:** MFA adds a second layer of security, even if a password is compromised.
- **Action steps:**
 - Turn on MFA for email, accounting, CRM, file storage, and other cloud platforms.
 - Use an authenticator app (like Microsoft Authenticator or Google Authenticator) rather than SMS where possible.
 - Require it as standard for all users, including external contractors.

3. Keep Software and Devices Updated

- **Why it Matters:** Outdated software and systems are a top entry point for cyber threats.
- **Action steps:**
 - Enable automatic updates for operating systems, browsers, antivirus, and business software.
 - Regularly check that all business devices (laptops, phones, tablets) are running current versions.
 - Don't ignore update prompts - they often patch critical security vulnerabilities.

4. Clean Up Outdated or Unused Data

- **Why it Matters:** Keeping unnecessary data increases risk and can breach data minimisation principles.
- **Action steps:**
 - Set up a regular schedule (e.g. quarterly) to delete or archive old files and records.
 - Remove data for contacts you no longer work with—clients, vendors, applicants, etc.
 - Only collect what you need. Don't store sensitive information "just in case."

5. Document and Communicate Your Privacy Policy

- **Why it Matters:** A clear, accessible policy shows you take data seriously—and helps you comply with NZ privacy laws.
- **Action steps:**
 - Make sure your policy outlines what data you collect, why, how it's stored, and who it's shared with.
 - Include how people can request access to or correction of their information.
 - Share the policy with staff and publish it on your website.

6. Train Your Team on Privacy Basics

- **Why it Matters:** People are your first line of defense, but only if they know what to watch for.
- **Action steps:**
 - Run a short training session (or share a 10-minute video) on password practices, phishing, and handling personal info.
 - Explain why privacy matters, not just the "what" but the "why."
 - Encourage staff to speak up if they notice anything unusual or concerning.

Ready to Get Started?

Download and print this checklist. Use it during your next team meeting or internal review. Tick off what you've done and plan what's next.

Want personalised advice or help implementing these steps?

Book a [free consultation](#) with our team. We're here to make data privacy easy.

